

1. A method for storing and withdrawing a decryption key from a key escrow database, comprising:

creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver;

randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token;

adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair;

encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair;

recording in a key escrow database the created set of N trap door encryption-decryption function pairs and the corresponding paired token;

recording in the key escrow database the randomly selected trap door encryption-decryption function pair along with the encrypted token; and

inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key.

2. A method for storing and withdrawing a decryption key from a key escrow database as in Claim 1, further comprising:

encrypting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door function along with the decryption key prior to recording in the key escrow database.

3. The method for storing and withdrawing a decryption key from a key escrow database as in Claim 1, further comprising:

randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token;

adding randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair;

concatenating the results of the adding of randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair to the corresponding token of the randomly selected first trap door encryption-decryption function pair; and

encrypting the concatenating results using the decryption key from the additional selected trap door encryption-decryption function pair.

B1  
cont  
4. The method for storing and withdrawing a decryption key from a key escrow database as in Claim 1 further comprising adding signature information at the receiver to the selected trap door encryption-decryption function pair to distinguish valid subsequent decodings of the selected trap door encryption-decryption function pair from invalid decodings.

5. The method for storing and withdrawing a decryption key from a key escrow database as in Claim 1, wherein encrypting the corresponding token of a selected trap door encryption-decryption function pair comprises calculating a cryptogram utilizing the corresponding token and including a decryption key along with randomization information and signature information.

6. A method for storing and withdrawing decryption keys from a key escrow database, comprising:

generating, in accordance with a selected encryption function, a set of  $N$  cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of  $N$  cryptogram/decryption key pairs and the corresponding token to a receiver;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key;

generating a cryptogram utilizing the corresponding decryption key and comprising the selected token and randomization information;

recording in an escrow database the generated set of  $N$  cryptogram/decryption key pairs along with each corresponding token and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; and

inverting the recorded set of  $N$  cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database.

BI cont  
7. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 6, further comprising:

randomly selecting at the receiver one or more additional  $N$  cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the corresponding token of the additionally selected encryption/decryption key pairs to identify a corresponding decryption key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding decryption key and comprising the selected additional token(s) and randomization information; and

mixing the token information from one selected key pair with the response cryptogram from a different selected key pair along with randomization information to diffuse response structure prior to generating another response cryptogram.

8. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 7, further comprising:

decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information.

9. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a linear transform.

10. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a symmetrical cryptosystem.

11. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 8 wherein mixing further comprises utilization of a public key cryptosystem.

12. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 6 wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs and a response message from the receiver prior to recording.

13. The method for storing and withdrawing decryption keys from a key escrow database as in Claim 12 further comprising adding signature information to the response message to enable valid decodings of the response message to be distinguished from invalid decodings.

14. A method for secure communication between an originator and a receiver using message encryption, comprising:

creating at an originator a set of N trap door functions each paired with a corresponding token, each trap door function comprising a cryptogram/decryption key pair;

transmitting the set of N trap door functions to a receiver;

randomly selecting at the receiver one of the trap door functions and the corresponding token;

adding at the receiver randomization information to the corresponding token of the selected trap door function;

encrypting at the receiver the decryption key with the randomly selected trap door function;

transmitting the encrypted decryption key with the randomly selected trap door function to the originator; and

decoding the encrypted decryption key with the randomly selected trap door function utilizing originator retained trap door information.

15. The method as in Claim 14 further comprising decrypting at the receiver the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair.

16. The method as in Claim 15 wherein encrypting at the receiver an escrow key comprises generating a cryptogram comprising the corresponding token, the decryption key and randomization information.

17. The method as in Claim 14 wherein decoding the encrypted escrow key comprises selecting a decryption key randomly from a selected group of decryption keys.

18. The method as in Claim 17 further comprising recognizing a correct decoding result utilizing structural information embedded in the response message.

19. The method as in Claim 14 wherein creating at an originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key.

20. The method as in Claim 14 further comprising:  
randomly selecting at the receiver an additional trap door function and the corresponding token;  
adding randomization information to the corresponding token of the additional selected trap door function;  
concatenating the results of the adding of the randomization information to the corresponding token of the additional selected trap door function to the encryption of the randomly selected first trap door function; and  
encrypting the concatenating results using the decryption key from the additional selected trap door function pair.

21. The method as in Claim 14 further comprising adding signature information at the receiver to the selected trap door function to distinguish valid subsequent decodings of the encrypted escrow key from invalid decodings.

22. The method as in Claim 14 further comprising:  
randomly selecting at the receiver one or more additional trap door functions and corresponding tokens;  
decrypting each cryptogram of the selected trap door functions utilizing the corresponding token of the additionally selected trap door functions to identify the corresponding decryption key for each additionally selected pair;  
adding at the receiver randomization information to the corresponding token of the additionally selected trap door functions;  
encrypting at the receiver an escrow key for each of the additionally selected trap door functions utilizing the corresponding description key and comprising the selected additional tokens and randomization information; and

mixing the token information from one selected trap door function with the encryption from a different selected trap door function along with randomization information to diffuse response structure prior to encrypting another trap door function.

23. The method as in Claim 22 wherein mixing comprises utilization of a symmetrical cryptosystem.

B1  
can't 24. The method as in Claim 22 wherein mixing further comprises utilization of a public key cryptosystem.

25. The method as in Claim 22 wherein mixing comprises utilization of a symmetrical cryptosystem.

26. The method as in Claim 14 further comprising recording in an escrow database the created N trap door functions along with each corresponding token and the encrypted escrow key with the randomly selected trap door function.

27. The method as in Claim 26 further comprising inverting the recorded set of N trap door functions and the encrypted escrow key with the randomly selected trap door function to identify a decryption key from the key escrow database.

---

Add the following new claims:

---

28. (New) A method for storing and withdrawing a decryption key from a key escrow database, comprising:

creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver;

randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token;

adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair;

encrypting with the selected trap door encryption-decryption function the token and the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair;

recording in a key escrow database the created set of N trap door encryption-decryption function pairs and the corresponding paired token;

recording in the key escrow database the randomly selected trap door encryption-decryption function pair along with the encrypted token and the added randomization information;

retrieving from the key escrow database the created set of N trap door encryption-decryption function pairs and the corresponding pair token, and the randomly selected trap door encryption-decryption function pair along with the encrypted token and the added randomization information; and

inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token and the added randomization information to identify the decryption key.



29. (New) A method for storing and withdrawing a decryption key from a key escrow database as in Claim 28, further comprising:

encrypting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door function along with the encrypted token and added randomization information prior to recording in the key escrow database.

30. (New) The method for storing and withdrawing a decryption key from a key escrow database as in Claim 28, further comprising:

randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token;

adding randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair;

concatenating the results of the adding of randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair to the corresponding token of the randomly selected first trap door encryption-decryption function pair; and

encrypting with the additional selected trap door encryption-decryption function pair the concatenating results.

31. (New) The method for storing and withdrawing a decryption key from a key escrow database as in Claim 28 further comprising adding signature information at the receiver to the selected trap door encryption-decryption function pair to distinguish valid subsequent decodings of the selected trap door encryption-decryption function pair from invalid decodings.

32. (New) The method for storing and withdrawing a decryption key from a key escrow database as in Claim 31, wherein encrypting the corresponding token of a selected trap door encryption-decryption function pair comprises calculating a cryptogram utilizing the corresponding token and including a decryption key along with randomization information and signature information.

33. (New) A method for storing and withdrawing decryption keys from a key escrow database, comprising:

generating, in accordance with a selected encryption function, a set of  $N$  cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of  $N$  cryptogram/decryption key pairs and the corresponding token to a receiver;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key;

generating a cryptogram utilizing the corresponding decryption key and comprising the selected token and randomization information;

recording in an escrow database the generated set of  $N$  cryptogram/decryption key pairs along with each corresponding token;

recording in an escrow database the generated cryptogram based on the randomly selected cryptogram/decryption key pair;

retrieving from the key escrow database the generated set of  $N$  cryptogram/decryption key pairs along with each corresponding token, and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; and

inverting the recorded set of  $N$  cryptogram/decryption key pairs and the generated cryptogram to identify a decryption key from the key escrow database.

34. (New) The method for storing and withdrawing decryption keys from a key escrow database as in Claim 33, further comprising:

randomly selecting at the receiver one or more additional  $N$  cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the corresponding token of the additionally selected encryption/decryption key pairs to identify a corresponding decryption key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding decryption key and comprising the selected additional token(s) and randomization information;

mixing the token information from one selected key pair with the response cryptogram from a different selected key pair along with randomization information to diffuse response structure prior to generating an additional response cryptogram; and

recording in an escrow database the generated additional response cryptogram.

B2  
cm't 35. (New) The method for storing and withdrawing decryption keys from a key escrow database as in Claim 33 wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs.

36. (New) The method for storing and withdrawing decryption keys from a key escrow database as in Claim 33 further comprising:

randomly selecting at the receiver an additional trap door function and the corresponding token;

adding randomization information to the corresponding token of the additional selected trap door function;

concatenating the results of the adding of the randomization information to the corresponding token of the additional selected trap door function to the encryption of the randomly selected first trap door function;

encrypting the concatenating results using the decryption key from the additional selected trap door function pair; and

recording in an escrow database the encrypted concatenating results using the decryption key from the additional selected trap door function pair.

---